REMARKS

The above amendments and these remarks are submitted in reply to the Office Action dated January 30, 2004.

By this Amendment, the specification has been amended to provide updated information regarding U.S. Patent Application Serial No. 09/404,298, as requested by the Examiner on page 2, paragraph 4 of the instant Office Action. Claims 1-2, 7-8, 13, 19-20, 25, 30-35, 37-39 and 44 have been amended. The Applicant submits that no new matter has been added by the aforementioned changes.

I. Objection to the Specification

The specification has been objected to for not including an update of the application recited on page 7, line 13 thereof. By this Amendment, the Applicant has provided the patent number of the recited application as suggested by the Examiner. Accordingly, reconsideration of the objection to the specification is respectfully requested.

II. Rejection of Claims 25-34

The Examiner has rejected Claims 25-34 under 35 U.S.C. §101 as being directed to non-statutory subject matter. By this Amendment, Claim 25 has been amended to be directed to a method, to make it consistent with dependent claims 26-29. Claims 30-34 have been amended to be directed to a calling program validation device. As such, the aforementioned claims are now submitted to be directed to statutory subject matter. Accordingly, reconsideration of the rejection of Claims 25-34 is respectfully requested.

III. Rejection of Claims 1-44

The Examiner has rejected Claims 1-44 under 35 U.S.C. §102(e) as being anticipated by Pearce (U.S. Patent No. 6,178,550). The Applicant traverses this rejection for the reasons set forth in greater detail below. The present invention is directed, for example, to a method for securely transferring control to system management mode (SMM) of a device after generation of a system management interrupt (SMI), and a

device that implements the secure transfer methodology. Claim 1 is directed to a secure transfer method including the following limitations:

> "...determining in SMM if the caller is included in a dispatch table..." and
>
> "...dispatching to a target function that is associated with the caller in the dispatch table if it is determined that the caller is included in the dispatch table..."

Such functionality, and the corresponding advantages provided thereby, are not disclosed or otherwise taught or suggested in Pearce. Consequently, Pearce does not anticipate the claimed invention. As disclosed, for example, on page 5, line 30, page 6, line 2, and as recited in the several claims of the present application, a caller refers to a portion of an executing program. Thus, a caller is part of the executing program, not a index or numerical parameter as recited in Pearce. In application, the present invention determines in system management mode (or a secure operating mode that uses a portion of memory or other applicable resources that are not accessible by the device operation system) if a calling portion of an executing program is present in a dispatch table, and dispatching execution to a target function associated with the caller. This functionality is not disclosed in Pearce.

As understood, Pearce is directed to a multi-table interrupt handling method where a function to be executed is determined (or indexed) by a corresponding index number that is provided by an interrupt (see, for example, col. 4, lines 43-45 and col. 4, lines 53-55). As clearly described, for example, at col. 4, lines 51-56, when an interrupt is received, one of the two tables (e.g. Jump Table) is searched to determine whether the specifically requested function (as identified by the received index number) is present in the jump table before the system enters system management mode. Thus, Pearce does not disclose "...determining in SMM if the caller is included in a dispatch table..." as defined in Claim 1.

Additionally, as the functions to be executed are determined by a received index value and not a portion of the program being executed, Pearce also does not determine "...if the caller is included in a dispatch table..." as defined in Claim 1. Consequently, as at least the aforementioned limitations are not disclosed or otherwise taught or suggested

in Pearce, the Applicant submits that Pearce does not anticipate the invention as defined in Claim 1.

An advantage provided by the present invention is increased efficiency in table searching and function execution. As clearly presented in Pearce, for example, at col. 4, lines 11-30, depending on the function requested, two tables: A BIOS Jump table and an SMM Jump table have to be linearly searched before a particular SMM function is executed. This is caused by the particular functions being associated with and identified by a specific function number. In contrast, the present invention employs a dispatch table, only accessible in SMM that correlates a caller with an associated function. As such, the dispatch table of the present invention may be traversed using binary search methodologies which are significantly faster than linear search techniques.

Another advantage provided by the present invention is that it provides a completely secure environment for transferring system or device control to SMM mode. Such security is provided by the fact that the function calls and corresponding function callers' locations are maintained in and are only accessible in SMM (see, for example, page 6, lines 16-20); thus, the functions are only accessible in a secure manner. This is in contrast to the teachings of Pearce, for example, col. 3, lines 45-47 and col. 4, lines 11-14, which state that functions indexed by a particular number or set of numbers "...may be implemented without regard to security..." Thus, it may be possible (according to the express teachings of Pearce) to crack or otherwise hack into the respective jump tables to emulate or potentially jeopardize system operation. In contradistinction, as the dispatch table of the present invention is only accessible in SMM, the ability to hack into the dispatch table is substantially reduced or eliminated.

Thus, as Pearce does not disclose each of the limitations provided in Claim 1 and the methodology presented in Pearce does not provide the security advantages of the present invention, the Applicant submits that Pearce does not anticipate the invention as defined in Claim 1. Accordingly, reconsideration of the rejection of Claim 1 is respectfully requested.

Claims 2-12 directly or indirectly depend upon and include all the limitations of Claim 1 and are submitted to be allowable at least for the reasons set forth above with respect to Claim 1. Moreover, these claims independently define novel subject matter as

compared to Pearce. For example, Claim 4 includes the limitation directed to "...exiting from SMM if it is determined that the caller is not included in the dispatch table..." As discussed in greater detail above, Pearce does not determine or disclose performing a caller check in system management mode. As discussed in Pearce, the function check is completed before the system enters (or is placed into) SMM. Thus, Pearce does not perform the function as recited in Claim 4, as the function search and check is performed before the system is placed in SMM. Accordingly, reconsideration of the rejection of Claims 1-12 is respectfully requested.

Like Claim 1, Claims 13 and 19, include limitations directed to "...determine in SMM if the caller is included in a dispatch table..." and "...dispatch to a target function that is associated with the caller in the dispatch table if it is determined that a caller is included in the dispatch table..." Thus, each of Claims 13 and 19 and the claims that directly and indirectly depend therefrom, are also allowable over Pearce. Accordingly, reconsideration of the rejection of Claims 13-24 is respectfully requested.

Claims 25, 30, 35 and 40 are directed to SMI interrupt validation methods and corresponding apparatus that include the following limitation;

> "...creating a dispatch table based on information associated with the predetermined indication, wherein each entry in the dispatch table associates a caller, which generates an SMI in the program, with a target function to be executed in system management mode (SMM)..."

that is not disclosed or otherwise taught or suggested in Pearce. Consequently, Pearce does not anticipate the invention as defined in the aforementioned claims. As discussed in greater detail above and as shown, for example, in Tables I and II of Pearce, the functions to be searched or performed, under a given circumstance, are not associated with a caller, as defined in the aforementioned claims; rather, they are associated with a function number within a prescribed range. Thus, Pearce does not disclose a system or method including a dispatch table with "...each entry in the dispatch table associated a caller, which generates an SMI in the program, with a target function to be executed in system management mode (SMM)..." Consequently, Pearce does not anticipate at least one limitation of the aforementioned claims. Accordingly, reconsideration of the rejection of Claims 25, 30, 35 and 40 is respectfully requested.

Claims 26-29, 31-34, 36-39 and 41-44 directly or indirectly depend upon and include the limitations of the aforementioned independent claims and are allowable at least for the reasons set forth above. Accordingly, reconsideration of the rejection of Claims 25-44 is respectfully requested.

IV. Rejection of Claims 28-29, 33-34, 38-39 and 43-44

The Examiner has rejected Claims 28-29, 33-34, 38-39 and 43-44 under 35 U.S.C. §103(a) as being unpatentable over Pearce in view of Srivastava (U.S. Patent No. 5,966,539). The Applicant traverses this rejection for the reasons set forth in greater detail below. Claims 28-29 directly or indirectly depend upon and include the limitations of Claim 25 and are allowable at least for the reasons set forth above with respect to Claim 25. Claims 33-34 directly or indirectly depend upon and include the limitations of Claim 30 and are allowable at least for the reasons set forth above with respect to Claim 30. Claims 38-39 directly or indirectly depend upon and include the limitations of Claim 35 and are allowable at least for the reasons set forth above with respect to Claim 35; and Claims 43-44 directly or indirectly depend upon and include the limitations of Claim 41 and are allowable at least for the reasons set forth above with respect to Claim 41.

As discussed above, Pearce does not disclose each and every limitation present in the corresponding independent claims of the present invention. Thus, Pearce does not anticipate the claimed invention. Adding Srivastava to the teachings of Pearce still does not render the claimed invention obvious as Srivastava does not overcome the deficiencies of Pearce as discussed in greater detail above. Thus, the combination of Pearce and Srivastava does not render the aforementioned claims obvious as submitted by the Examiner. Accordingly, reconsideration of the rejection of Claims 28-29, 33-34, 38-39 and 43-44 is respectfully requested.

CONCLUSION

In view of the above amendments and remarks, it is respectfully submitted that Claims 1-44 are now in proper condition for allowance and such action is earnestly solicited.

The Commissioner is hereby authorized to charge any underpayments or credit any over payments to Deposit Account No. 16-1520 for any payment in connection with this communication, including any fees for extension of time, which may be required. The Examiner is invited to call the undersigned if such action might expedite the prosecution of this application.

Respectfully submitted,
PHOENIX TECHNOLOGIES LTD.

Date: July 30, 2004

By: _____
Loren H. McRoss
Registration No. 40,427

915 Murphy Ranch Road
Milpitas, CA 95035
PH: (408) 570-1000
FX: (408) 570-1044